

E-5272-01EK

A METHOD FOR MANAGING PUBLIC KEY

002090"85E8560

BACKGROUND OF THE INVENTION

本発明は、公開鍵の管理方法に係り、特に、ネットワークにおけるセキュリティ技術に使用される公開鍵暗号システムに使用して好適な公開鍵の管理方法に関する。

インターネットを使用してセキュリティ通信を実現する方法として、例えば、IP (Internet Protocol) レイヤのセキュリティプロトコルである IPSEC (IP SECurity) がある。IPSEC に関する技術文献として、例えば、IETF (Internet Engineering Task Force) 発行の [RFC1825] “Security Architecture for the Internet Protocol.” (R. Atkinson 著) 等が知られている。

IPSEC に付随する鍵管理プロトコルは、公開鍵暗号システムを利用するものである。鍵管理プロトコルに関する従来技術として、例えば IETF 発行の “Simple Key-Management For Internet Protocol.” (著者: Ashar Aziz, Tom Markson, Hemma Prafullchandra) 等に記載された SKIP と呼ばれる技術が知られている。以下、この鍵管理プロトコルについて説明する。

いま、ネットワーク内にセキュリティ通信を行う 2 つのホスト A、B があり、これらのホスト A、B は、IPSEC に基づいた共通鍵暗号システムによって暗号通信を行うものとし、ホスト A は、ホスト B の公開鍵を、ホスト B は、ホスト A の公開鍵を知っているものとする。

ホスト A と B とは、通信を行うに際して、既知のアルゴリズムを用いてそれぞれ自らの秘密鍵と相手の公開鍵とを組み合わせることで共通鍵を暗号化するための鍵 $K(A)$ 、 $K(B)$ を生成する。ここで、例えば、ホスト A がホスト B にデータを送信するとき、ホスト A は、共通鍵 T を生成し、それを用いてデータを暗号化し、鍵 $K(A)$ を用いて共通鍵 T を暗号化する。ホスト A は、暗号化された共通鍵 T の情報を含む新たなヘッ

前述したようなIPSECに付随する従来技術による鍵管理プロトコルは、セキュリティ通信を行う2つのホストが通信開始前に互いに相手の公開鍵を知っていることが前提とされている。

前述した従来技術による方法は、セキュリティ通信を行おうとする2つのホストが、通信開始前にお互いの公開鍵を自動的かつ安全に交換する方法がなく、その結果、手渡しによる公開鍵の交換等の方法に頼ることになり、公開鍵の管理が複雑になっているという問題点を有している。また、この結果、前述の従来技術は、ネットワークの規模が大きい場合、ネットワークの管理者に対する負担が大きくなるという問題点を生じさせている。

さらに、前述の従来技術は、ネットワーク上の認証を伴わない公開鍵の配布を行った場合、不正なホストがセキュリティ通信の相手になりすますことを防ぐことができないという問題点をも有している。

SUMMARY OF THE INVENTION

本発明の目的は、前述した従来技術の問題点を解決し、セキュリティ通信を行おうとする２つのホストが通信開始前にお互いの公開鍵を自動的にかつ安全に交換することを可能にした公開鍵の管理技術を提供することにある。

本発明によれば前記目的は、階層構造を持ち、各階層毎にドメイン名を持つネットワークと、そのドメイン名とアドレスとの対応を管理する前記各階層毎に設けられるDNSサーバと、ネットワークに収容されるホストとを備え、前記DNSサーバが、ネットワークに属するホストに対して他のホストが持つ公開鍵を配布する公開鍵管理システムにおいて、前記DNSサーバが、公開鍵を管理する手段と、前記ネットワ

ークに属するホストの公開鍵とドメイン名とを対応付けて格納するデータベースとを備え、第1のホストからのドメイン名の情報による第2のホストの公開鍵の問い合わせを受けたとき、前記公開鍵管理手段が前記データベースを参照することにより、前記ドメイン名に対応する第2のホストの公開鍵の情報を前記第1のホストに応答することにより達成される。

また、前記目的は、前記DNSサーバが、第1のホストから第2のホストの公開鍵の問い合わせを受けたとき、自サーバ内の前記データベースの中に問い合わせのドメイン名に対応するエントリがない場合、他の公開鍵管理手段とデータベースとを備えた他のDNSサーバに公開鍵の解決をドメイン名の階層に沿って再帰的に委託することにより達成される。

さらに、前記目的は、前記ホストが、前記DNSサーバに他のホストの公開鍵を問い合わせる手段を備え、セキュリティ通信開始時、前記公開鍵問い合わせ手段に通信相手となるホストのドメイン名に対応する公開鍵を前記DNSサーバに問い合わせることにより達成される。

本発明の目的は、前述の手段を持つ構成以外に、さらに、次に示すような手段を備えることによっても達成することができる。

すなわち、前記目的は、ネットワークの構成に変更が生じた場合、構成の変化に関係する一部のDNSサーバが、ホストの公開鍵とドメイン名のと対応を格納しているデータベースを更新し、前記以外のDNSサーバがデータベースの更新を行わないようにすることにより達成される。

また、前記目的は、前記公開鍵管理手段とデータベースとを備えたDNSサーバと、前記公開鍵を問い合わせる手段を備えたホストとに電子署名を処理する手段を設け、公開鍵問い合わせ及び応答のために出力するパケットに電子署名を付け、電子署名の付いた入力パケットについて、その電子署名を確認し、改竄されている入力パケットを廃棄することにより、パケットの内容が改竄されるのを防止することにより達成される。

また、前記目的は、公開鍵問い合わせ及び応答のために上記公開鍵管理手段とデータベースとを備えたDNSサーバと、前記公開鍵を問い合わせる手段を備えたホストとが、入出力するパケットとして、従来のDNSパケットと同じフォーマットのパケットを用いることにより達成される。

また、前記目的は、前記DNSサーバに対してホストが送信する公開鍵問い合わせパケットの中にホストが信用するDNSサーバのドメイン名の情報を含め、公開鍵の情報を応答する前に、前記DNSサーバの公開鍵管理手段に、公開鍵問い合わせパケットの中で示されるホストが信用するDNSサーバに対して電子署名を要求させ、電子署名の要求を受けたDNSサーバの公開鍵管理手段に、公開鍵応答パケットに電子署名を付けさせ、その電子署名により公開鍵応答パケットに含まれる公開鍵の情報が信用できるか否かを前記ホストの電子署名を処理する手段に判定させ、これにより、不正なホストが自分の公開鍵とアドレスとを公開鍵問い合わせパケットの中にある問い合わせドメイン名に対応しているように見せかけることを防止するようにしたことにより達成される。

また、前記目的は、電子署名の要求を受けたDNSサーバが公開鍵問い合わせパケットの中で示されるホストが信用するDNSサーバと異なるとき該DNSサーバの公開鍵管理手段は、ドメイン名の階層構造に沿って、上位のDNSサーバに公開鍵応答パケットに対する電子署名を要求し、最終的には公開鍵問い合わせパケットの中で示されるホストが信用するDNSサーバに公開鍵応答パケットに電子署名を付けさせることにより達成される。

また、前記目的は、前記ホストの公開鍵問い合わせ手段に、問い合わせるドメイン名に従って信用するDNSサーバを選択させ、公開鍵問い合わせパケットの中に該DNSサーバのドメイン名の情報を含め、公開鍵応答パケットに電子署名を付ける処理を行うDNSサーバの数を減らすことにより公開鍵の取得を効率的なものとすることにより達成される。

また、前記目的は、電子署名付きの公開鍵の応答を受けたDNSサーバの公開鍵

[illegible]

図2は上記実施形態におけるDNSクライアントの機能を持つホストの構成を示すブロック図である。

図3は上記実施形態における公開鍵とドメイン名との対応を説明するテーブルの構成を示す図である。

図4はDNSサーバが公開鍵の問い合わせを受けたときに公開鍵を応答する手順を説明するフローチャートである。

図5はDNSサーバが電子署名の要求を受けたときに公開鍵応答パケットに電子署名を付与する手順を説明するフローチャートである。

図6はDNSクライアントの機能を持つホストが通信相手の公開鍵を取得する手順を説明するフローチャートである。

図7は本発明を階層的なドメイン名の構造を持つネットワークに適用した場合の実施形態を示すブロック図である。

図 8 はホストが通信相手の公開鍵の取得ために行う手順の中で、ホスト・KMS 間及び KMS・KMS 間でやり取りするパケットの種類とそれらに付与される電子署名を説明する図である。

図9はDNSパケットのフォーマットの構成を説明する図である。

図10はDNSパケットに含まれる資源レコードのフォーマットの構成を説明する図である。

以下、本発明を用いた公開鍵管理システムの実施形態を図面を参照して詳細に説明する。

図1は本発明の一実施形態の公開鍵管理システムにおけるKMS (Key Management Server)の構成を示すブロック図、図2はDNSクライアントの機能を持つホストの構成を示すブロック図である。KMSはDNSサーバを機能拡張したサーバである。同様に、上記ホストは機能拡張したDNSクライアントの機能を持つ。図3は公開鍵とドメイン名との対応を説明するテーブルの構成を示す図、図4はDNSサーバが公開鍵の問い合わせを受けたときに公開鍵を応答する手順を説明するフローチャート、図5はDNSサーバが電子署名の要求を受けたときに公開鍵応答パケットに電子署名を付与する手順を説明するフローチャート、図6はDNSクライアントの機能を持つホストが通信相手の公開鍵を取得する手順を説明するフローチャート、図7は本発明を階層的なドメイン名の構造を持つネットワークに適用した場合の実施形態を示すブロック図、図8はホストが通信相手の公開鍵の取得ために行う手順の中で、ホスト・KMS間及びKMS・KMS間でやり取りするパケットの種類とそれらに付与される電子署名を説明する図、図9はDNSパケットのフォーマットの構成を説明する図、図10はDNSパケットに含まれる資源レコードのフォーマットの構成を説明する図である。図1、図2、図7、図8において、10はKMS、11、21はネットワーク制御部、12、22はIP処理部、13、23はTCP/UDP処理部、14は拡張DNS処理部、15はドメイン名/IPアドレステーブル、16、25はドメイン名・公開鍵・電子署名テーブル、17、26は初期保持データ、24は拡張DNSクライアント、27はセキュリティ通信処理部、101はネットワーク、141、241はDNSパケット振り分け部、142はDNS処理部、143は公開鍵問い合わせ/応答処理部、144は電子署名処理部、242はドメイン名リゾルバ、243は公開鍵問い合わせ処理部、244は電子署名処理部、71、75はホストA、B、72～74、76はKMSである。

まず最初に、本発明が適用されるネットワークシステム全体の構成及び処理の流れについて図7を参照して説明する。

図7に示すネットワークシステムは、ネットワークが階層構造を持ち、各階層毎

にドメイン名が与えられており、ドメインを持つネットワークの各階層が1つのKMSを持つように構成されている。ここで、ホストA 7 1がホストB 7 5の公開鍵を取得する場合について考える。この場合、ホストA 7 1は、同一のドメインの階層にあるKMS 1 (7 2)に対してホストB 7 5の公開鍵を問い合わせる。このとき、単にホストB 7 5の公開鍵のデータを受け取るのみでは不正な他のホストがホストB 7 5に成りすますのを防ぐことができないので、ホストA 7 1は、信用することができるKMSの電子署名も要求する。今の場合、ホストA 7 1が信用するKMSはKMS 0 0 (7 4)であるとする。また、KMS 0 0 (7 4)の公開鍵は、ホストA 7 1のみならず一般に広く知られ、認証されているものとする。

ホストA 7 1がホストB 7 5の公開鍵のデータを要求すると、KMS 1 (7 2)はこの要求に対して、ホストB 7 5の公開鍵のデータを持っている場合、ホストA 7 1が信用しているKMS 0 0 (7 4)にホストB 7 5の公開鍵のデータに電子署名を付けるように要求する。一方、KMS 1 (7 2)は、ホストB 7 5の公開鍵のデータを持ってない場合、上位のKMS 0 (7 3)に問い合わせる。その際、ホストB 7 5の公開鍵のデータを持っているKMSに行き会うまで再帰的に上位のKMSへの問い合わせが続けられる。KMS 1 (7 2)からの問い合わせを受けたホストB 7 5の公開鍵のデータを持っているKMSは、KMS 0 0 (7 4)に電子署名を要求する。

電子署名を付けるように要求されたKMS 0 0 (7 4)は、自らの電子署名を付けたホストB 7 5の公開鍵のデータをKMS 1 (7 2)に返す。KMS 1 (7 2)は、ホストB 7 5の公開鍵のデータをホストA 7 1に返す。この場合、ホストA 7 1は、元々KMS 0 0 (7 4)の公開鍵を知っているためそれが信用できるデータか否かを判断することができる。

前述した一連の処理によりホストA 7 1は、ホストB 7 5の公開鍵を安全に取得することができ、これを使用して、ホストB 7 5との間でセキュリティ通信を行うことができる。

次に、図9、図10を参照して、DNSパケットのフォーマットの構成と、DN

S パケットに含まれる資源レコードのフォーマットの構成とを説明する。

DNS パケットは、図 9 に示すように、DNS ヘッダ 9 1、問い合わせ部 9 2、回答部 9 3、権限付きネームサーバの名前を表す権威部 9 4、複数の資源レコードを含む付加情報部 9 5 から成る。また、図 10 に示すように、DNS パケットに含まれる資源レコードの 1 つである TXT レコードは、名前フィールド 1 0 1、TYPE フィールド 1 0 2、CLASS フィールド 1 0 3、この資源レコードが捨てられずにキャッシュされている時間間隔を示す TTL フィールド 1 0 4、データ長フィールド 1 0 5、データフィールド 1 0 6 からなる。

複数の資源レコードとしては、TYPE により識別される複数のものがあり、本発明の実施形態においては、複数ある DNS 資源レコードの内 TXT レコードと呼ばれる TYPE = 1 6 の資源レコードに、公開鍵問い合わせ情報及び公開鍵応答情報を入れることとする。また、本発明の実施形態は、公開鍵問い合わせ情報及び公開鍵応答情報を入れる資源レコードのデータフィールド 1 0 6 の先頭に公開鍵問い合わせ／応答、電子署名要求、または、通常の TXT レコードの区別がつくような識別子 1 0 6 1 のフィールドを設けている。

なお、TXT レコードについては、前掲の DNS に関する文献の中に説明がある。また、資源レコードとして、前述した TXT レコードの他に、アドレスとドメイン名との対応を示す A レコード (TYPE = 1)、メール・エクスチェンジャのドメイン名を示す MX レコード (TYPE = 1 5) 等がある。

次に、図 1 を参照して、本発明の実施形態によるサーバである KMS の構成を説明する。図 1 において、各ブロックを結ぶ実線はパケットの受け渡しを行う関係を示し、破線はデータの参照を行うことを示す。

KMS 1 0 は、ネットワーク制御部 1 1 と、IP 処理部 1 2 と、TCP/UDP 処理部 1 3 と、拡張 DNS 処理部 1 4 と、ドメイン名・IP アドレステーブル 1 5 と、ドメイン名・公開鍵・電子署名テーブル 1 6 と、初期保持データ 1 7 とを備えて構成され、ネットワーク制御部 1 1 を介してネットワーク 1 0 1 に接続されている。また、

目を含む。公開鍵問い合わせ／応答処理部143は、もし、ドメイン名・公開鍵・電子署名テーブル16にエントリがあれば、問い合わせの要求に従って他のKMSへ電子署名の要求を出すか、または、電子署名処理部144によって公開鍵の応答パケットに電子署名を付ける処理を行う。また、公開鍵問い合わせ／応答処理部143は、ドメイン名・公開鍵・電子署名テーブル16にエントリがないとき、TCP／UDP処理部13を介して他のKMSに対して、問い合わせのあったドメイン名の公開鍵を問い合わせるパケットを送信する。電子署名処理部144は、他のKMSからの電子署名要求を拡張DNSパケットの形でTCP／UDP処理部13から受け取ったとき、問い合わせの要求に従って他のKMSへ電子署名の要求を出すか、または、公開鍵応答パケットに電子署名を付ける処理を行う。

また、KMS10は、初期保持データ17を保持している。初期保持データ17は、自分のドメイン名・公開鍵171、DNSの親子関係において上位のKMSのドメイン名172、DNSの親子関係において下位にあるものの中で信用するKMSのドメイン名・公開鍵173から成る。KMS10は、他のKMSに公開鍵を問い合わせに行くときにこれらのデータを利用する。

次に、図2を参照して本発明により拡張したDNSクライアントの機能を持つホストの構成を説明する。

ホスト20は、ネットワーク制御部21と、IP処理部22と、TCP／UDP処理部23と、拡張DNSクライアント24と、ドメイン名・公開鍵・電子署名テーブル25と、初期保持データ26と、セキュリティ通信処理部27とを備えて構成され、ネットワーク制御部11を介してIPネットワーク101に接続されている。また、拡張DNSクライアント24は、DNSパケット振り分け部241と、ドメイン名リゾルバ242と、公開鍵問い合わせ処理部243と、電子署名確認部244とを備えて構成されている。

前述において、ホスト20は、KMSと同様に、ネットワーク制御部21、IP処理部22、TCP／UDP処理部23を持ち、IPネットワーク201に接続され

ている。TCP/UDP処理部23は、DNSに割り当てられたソケット番号を持つパケットを受信したとき、そのパケットを拡張DNSクライアント24に送る。逆に、拡張DNSクライアント24は、自ら生成したパケットを送信するとき、そのパケットをTCP/UDP処理部23に送る。

拡張DNSクライアント24内のDNSパケット振り分け部241は、TCP/UDP処理部23からDNSパケットを受け取り、DNSヘッダの中身を見てドメイン名リゾルバ242、公開鍵問い合わせ処理部243のいずれかに処理を振り分ける。ドメイン名リゾルバ242は、従来のDNSクライアントと同様に、ドメイン名に対応するIPアドレスを解決する処理を行う。そして、ドメイン名に対応するIPアドレスを問い合わせる際、ドメイン名リゾルバ242は、TCP/UDP処理部23を通して問い合わせパケットを送信する。ドメイン名リゾルバ242は、問い合わせに対する応答もTCP/UDP処理部23を通して受信する。

本発明により新たに付加したモジュールである公開鍵問い合わせ処理部243は、ドメイン名に対応する公開鍵を解決する処理を行う。公開鍵問い合わせ処理部243は、新規に得た公開鍵の情報をドメイン名・公開鍵・電子署名テーブル25に保存し、次回に公開鍵を問い合わせに行く前に参照する。電子署名確認部244は、公開鍵問い合わせ処理部243が受け取った公開鍵の情報について、初期保持データ26内の信用するKMSのドメイン名・公開鍵263を参照して、公開鍵の情報に付いている電子署名が信用するKMSのものか否かを判定し、公開鍵の情報が信用できるか否かを確認する。

公開鍵問い合わせ処理部243は、信用するKMSのドメイン名・公開鍵263が複数ある場合に、公開鍵を問い合わせるドメイン名に応じて信用するKMSのドメイン名・公開鍵263の中から最適な信用するKMSを選択する。ホスト20は、初期保持データ26内に自分のドメイン名・公開鍵261と上位のKMSのドメイン名262とを持ち、公開鍵問い合わせ処理部243は、公開鍵を問い合わせに行く際に自分のドメイン名・公開鍵261と上位のKMSのドメイン名262とを参照する。

セキュリティ通信処理部27は、公開鍵問い合わせ処理部243が取得した通信相手の公開鍵に基づいて、従来の方法に従ってセキュリティ通信を行う。

次に、図4に示すフロー、及び、ホスト・KMS間及びKMS・KMS間でやり取りするパケットの種類とそれらに付与される電子署名を示す図8を参照して、本発明を階層的なドメイン名の構造を持つネットワークに適用した場合の図7に示すネットワークにおいて、ホストが通信相手の公開鍵の取得ために行う手順について説明する。

図7において、KMS0(73)、KMS1(72)、KMS2(76)、KMS00(74)は、図1により説明した構成を持つKMSであり、また、ホストA71、B75は、図2により説明した構成の拡張したDNSクライアントの機能を持つホストである。そして、KMS00(74)は、ドメイン名xxを持つネットワーク701に接続され、KMS0(73)は、ドメイン名a.xxを持つネットワーク702に接続されている。また、ホストA71とKMS1(72)とは、ドメイン名b.a.xxを持つネットワーク703に接続され、ホストB75とKMS2(76)とは、ドメイン名c.a.xxを持つネットワーク704に接続されている。

ドメイン名は、階層構造を成しており、各KMSは、従来のDNSサーバの役割をも果たしている。また、図8に示す例は、ホストB75の公開鍵の情報をKMS2(76)のみが持っている場合の各KMSの動作を示しており、また、図8に示す各矢印は、ホストA71がホストB75の公開鍵を取得する際に、ホストとKMSとの間やKMSとKMSとの間でやり取りするパケットやパケットに付加する電子署名の形態を示している。パケットの種類は、公開鍵問い合わせ、電子署名要求、公開鍵応答の3通りあり、電子署名の具体的な内容は、図8の枠内の記号を用いて表しているように、次のように定義されているものとする。

S(K, [a, b, c]) : 鍵Kによりメッセージ[a, b, c]に電子署名
を付与したもの

D(X) : Xのドメイン名

S (X) : Xの公開鍵

T (X) : Xの秘密鍵

IP (X) : XのIPアドレス

KMS (X) : Xが電子署名を要求するKMS

以下、ホストA 7 1が電子署名を要求するKMSがKMS 0 0 (7 4)であるとして図4に示すフローを説明する。

(1) まず、ホストAは、ホストB 7 5の公開鍵を問い合わせるパケットをKMS 1 (7 2)に送信する。この公開鍵を問い合わせるパケットは、図8に矢印8 1により示しているように、

S (T (A) , [D (B) , KMS (A) , IP (A) , D (A)])

であり、これは、前述の定義から理解できるように、ホストBのドメイン名、ホストAが電子署名を要求するKMS、ホストAのIPアドレス、ホストAのドメイン名よりなるメッセージに、ホストAの秘密鍵により電子署名を行ったものである。KMS 1 (7 2)がホストA 7 1からホストB 7 5の公開鍵を問い合わせるパケットを受けるとき、図1に示す電子署名処理部1 4 4は、パケットに付いている電子署名を見る。電子署名処理部1 4 4は、ドメイン名・公開鍵・電子署名テーブル1 6からホストA 7 1の公開鍵を取り出し、パケットの内容が改竄されていないか否かをその公開鍵を使って判定する(ステップ4 1)。

(2) KMS 1 (7 2)は、ステップ4 1の判定で、問い合わせパケットが改竄されていた場合、そのパケットを廃棄して処理を終了し、問い合わせパケットが改竄されていない場合、図1に示す公開鍵問い合わせ/応答処理部1 4 3を動作させ、問い合わせのドメイン名についてドメイン名・公開鍵・電子署名テーブル1 6にエントリがあるか否か検索する。ここで、タイムスタンプも参照し、一定時間以上過ぎている場合、無効なエントリと見做す(ステップ4 3、4 2)。

(3) ステップ4 2の判定で、ドメイン名・公開鍵・電子署名テーブル1 6にエントリがなかったとき、図7に示すKMS 1 (7 2)の公開鍵問い合わせ/応答処理部1 4

3は、問い合わせのあったホストのドメイン名と自分のドメイン名とについてそれぞれが属するネットワークの名前が一致するか否かを判定する。例えば、図7において、問い合わせのホストがB 7 5である場合、B 7 5の属するネットワークのドメイン名c. a. x xとKMS 1 (7 2)の属するネットワークのドメイン名b. a. x xは一致しない(ステップ4 4)。

(4) ステップ44の判定においてネットワークの名前が一致したとき、図7のKMS1(72)は、ホストA71に対してホストBに対する公開鍵が未解決であることを通知する(ステップ45)。

(5) ステップ44の判定においてネットワークの名前が一致しなかったとき、KMS1(72)は、図1にける初期保持データ17内の上位のKMSのドメイン名172を参照して問い合わせ先を調べ、KMS0(73)にホストB75の公開鍵を問い合わせる。この場合の問い合わせパケットは、図8に矢印82により示すように、

S(T(KMS 1), [D(B), KMS(A), IP(KMS 1), D(KMS 1)])で
あり、ホストB 7 5のドメイン名、ホストA 7 1が電子署名を要求するKMSのド
メイン名、KMS 1(7 2)のIPアドレス及びKMS 1(7 2)のドメイン名をメッセ
ージとし、KMS 1(7 2)の秘密鍵を電子署名の鍵とする電子署名を付加して構成され
る。このように、電子署名を付加することによって問い合わせパケットの不正な改竄
を防止することができる(ステップ4 6)。

(6) 次に、KMS 1 (7 2) は、自 KMS に公開鍵を問い合わせた者がホストか KMS かを公開鍵問い合わせパケットの始点 IP アドレスから判定し、公開鍵を問い合わせたのが KMS である場合、処理を終了する (ステップ 4 6 1)。

(7) ステップ461で、自KMSに公開鍵を問い合わせた者がホストである場合、公開鍵問い合わせ／応答処理部143は、上位のKMSから公開鍵の応答があるまで一定時間待ち、一定時間内に公開鍵の応答がなく、電子署名付きの公開鍵を取得できなかった場合、処理を終了する(ステップ462、463)。

(8) 公開鍵問い合わせ／応答処理部 143 は、電子署名付きの公開鍵の応答が一定

時間内にあった場合、その公開鍵を図 1 に示すドメイン名・公開鍵・電子署名テーブル 1 6 にキャッシングする。このようにキャッシングを行うことにより、別のホストから同じドメイン名について公開鍵の問い合わせがあったときに、公開鍵問い合わせ／応答処理部 1 4 3 は、再度別の KMS に公開鍵の問い合わせに行かずに済み、公開鍵を解決する処理を効率的に行うことができる（ステップ 4 6 4）。

(9) 次に、公開鍵問い合わせ／応答処理部 143 は、図 8 の矢印 87 に示すように自らの電子署名をつけた公開鍵応答パケットを公開鍵の問い合わせを受けたホストに返す。この電子署名付きの公開鍵応答パケットは、 $D(KMS1)$ 、 $D(B)$ 、 $S(B)$ 、 $S(T(KMS00))$ 、 $[D(B), S(B), D(KMS00)]$ をメッセージとし、秘密鍵 $T(KMS1)$ を署名の鍵とするものである（ステップ 465）。

(10) ステップ42のデータベースの検索で、問い合わせのドメイン名について、ドメイン名・公開鍵・電子署名テーブル16にエントリがあった場合、図1に示す公開鍵問い合わせ／応答処理部143は、そのエントリに指定されたKMSの電子署名が付いているか否かを見る(ステップ47)。

(11) ステップ 47 のチェックで、指定された KMS の電子署名がエントリに付いていた場合、公開鍵問い合わせ／応答処理部 143 は、そのエントリにある電子署名付きの公開鍵をホスト A71 に返す（ステップ 48）。

(12) 一方、ステップ47で指定されたKMSの電子署名がエントリに付いていなかった場合、公開鍵問い合わせ／応答処理部143は、パケットに付いているホストA71が信用するKMSと図1の初期保持データの上位のKMSのドメイン名172を見て、図7に示すKMS0(73)に電子署名の要求を出す。図7に示すKMS2(76)がホストB75の公開鍵の情報を持っていて、KMS0(73)に電子署名の要求を出す場合、図8の矢印84に示すように、[D(B)、KMS(A)、IP(KMS1)、S(B)及びD(KMS2)]をメッセージとして、KMS2(76)の秘密鍵を鍵とする電子署名を付けて要求を行う(ステップ49)。

前述では、図 7 における KMS 1 (7 2) の動作について説明したが、他の KMS

次に、図5に示すフローと図7及び図8とを参照して、図1に示すKMSの各部の動作の中での電子署名の要求と応答とについて説明する。

(1) いま、図7に示すKMS0(73)が、KMS1(72)から電子署名の要求を受けたとする。この場合、KMS0(73)は、図1に示ような構成を持つ自装置内の電子署名処理部144を動作させ、パケットに付いている電子署名を見る。電子署名処理部144は、ドメイン名・公開鍵・電子署名テーブル16からKMS172の公開鍵を取り出し、パケットの内容が改竄されていないか否かを判定する(ステップ51)。

2) ステップ5 1の判定で、パケットの内容が改竄されていた場合、電子署名処理部1 4 4はパケットを廃棄し、KMS 0(7 3)は処理を終了する(ステップ5 3)。

(3) ステップ51の判定で、パケットの内容が改竄されていなかった場合、電子署名処理部144は、パケットの内容を見て電子署名の要求先が自分自身か否かを判定する(ステップ52)。

(4) ステップ52の判定で、電子署名の要求先が自分自身でない場合、電子署名処理部144は、初期保持データの上位のKMSのドメイン名172を参照し、電子署名の要求を上位のKMSに対して出す。図7において、ホストA71が電子署名を要求するKMSがKMS00(74)である場合、図8の矢印85に示すように、KMS0(73)からKMS00(74)への電子署名要求パケットは、[D(B)、KMS(A)、IP(KMS1)、S(B)及びD(KMS0)]をメッセージとしKMS0(73)の秘密鍵を鍵とする電子署名を付けたものとなる(ステップ54)。

(5) 一方、ステップ52の判定で、電子署名の要求先が自分自身であった場合、電子署名処理部144は、要求されたパケットに対して自分の秘密鍵によって電子署名を付け、要求元のKMSに電子署名付きのパケットを返す。説明している例で、例えば、署名要求に対してKMS00(74)がKMS1(72)へ公開鍵を応答するものとする、その場合の応答パケットは、図8の矢印86に示すように、[D(B)、S(B)及びD(KMS00)]をメッセージとしKMS00(74)の秘密鍵を鍵とする。

る電子署名を付けたものとなる（ステップ55）。

次に、図6に示すフローと図7及び図8とを参照して、図2に示す構成のホストの動作を説明する。

(1) 図7において、ホストA71がホストB75の公開鍵を取得しようとするものとする。このとき、図2に示す構成を持つホストA71の公開鍵問い合わせ処理部243は、ドメイン名・公開鍵・電子署名テーブル25を検索しホストB75のエントリがあるか否かを調べる(ステップ61)。

(2) ステップ61で、ドメイン名・公開鍵・電子署名テーブル25にホストB75のエントリがなかったとき、公開鍵問い合わせ処理部243は、初期保持データ26の信用するKMSのドメイン名・公開鍵263を参照して信用するKMSを選択し、信用するKMSのドメイン名・公開鍵263が複数ある場合、問い合わせるドメイン名より上位にあってそれに最も近いKMSを選択する(ステップ62)。

(3) 次に、公開鍵問い合わせ処理部243は、初期保持データ26内の公開鍵を問い合わせに行くKMSのドメイン名262を参照して、そのKMSにホストB75の公開鍵を問い合わせる。この場合の公開鍵問い合わせパケットは、図8の矢印81に示すように、[D(B)、KMS(A)、IP(A)及びD(A)]をメッセージとし、ホストAの秘密鍵T(A)を鍵とする電子署名を付加したものとなる(ステップ63)。

(4) ホストA 7 1は、ステップ6 3での問合せに対して、公開鍵応答パケットが返ってきたとき、図2の電子署名確認部2 4 4を動作させ、公開鍵応答パケットに付いている電子署名が要求したKMSのものであって、かつパケットの内容が改竄されていないかを確認する(ステップ6 4)。

(5) 一定時間以内に公開鍵応答パケットが返ってこないとき、あるいは、ステップ 64 で、公開鍵応答パケットに付いている電子署名が要求した KMS のものでないか、パケットの内容が改竄されていると判定された場合、ホスト A 71 は、何もせずに処理を終了する。これにより、ネットワーク上にある不正なホストが自らの公開鍵とア

ドレスが問い合わせのあったドメイン名に対応しているように見せかけることでセキュリティ通信の相手になりすますことを防止することができる。

(6) ステップ64で、公開鍵応答パケットに付いている電子署名が要求したKMSのものであって、かつパケットの内容が改竄されていないと判定された場合、公開鍵問い合わせ処理部243は、その公開鍵応答パケットの内容を見て、ドメイン名・公開鍵・電子署名・署名したKMSのドメイン名の4つの組でドメイン名・公開鍵・電子署名テーブル25にキャッシングする(ステップ65)。

(7) ホストA71のセキュリティ通信処理部27は、前述までの処理で取得した公開鍵、あるいは、ステップ61で見つかった公開鍵を用い、セキュリティ通信を行うための処理を開始する(ステップ66)。

ホストは、前述した処理を実行することにより、公開鍵を解決する処理を効率化することができる。

前述した本発明の実施形態によれば、ネットワークの2つのホストがセキュリティ通信を開始する前に機能拡張したDNSサーバによって通信相手のホストのドメイン名に対応する公開鍵を自動的に取得させることが可能となり、公開鍵の管理の容易化を図ることができる。

また、本発明の実施形態によれば、ホストが指定したDNSサーバによって公開鍵の応答パケットに電子署名を付けさせることができるので、ネットワーク上にある不正なホストが自らの公開鍵とアドレスとが問い合わせのあったドメイン名に対応しているように見せかけることによりセキュリティ通信の相手になりすますことを防止することができる。

前述したような本発明は、FDやCD-ROM等の記憶媒体に本発明を実現するプログラムを格納しておき、このプログラムをDNSサーバ及びホストにインストールして実現することができる。また、本発明は、ネットワークに接続された情報処理装置の記憶媒体に本発明を実現するプログラムを格納しておき、ネットワークを通してDNSサーバ及びホストのハードディスク等の記憶媒体に前述のプログラムをコ

ピーして実現することができる。

002090 85E58560

CLAIMS

1. 階層構造を持ち、各階層毎にドメイン名を持つネットワークと、そのドメイン名とアドレスとの対応を管理する前記各階層毎に設けられるDNSサーバと、ネットワークに収容されるホストとを備え、前記DNSサーバが、ネットワークに属するホストに対して他のホストが持つ公開鍵を配布する公開鍵管理方法において、前記DNSサーバは、公開鍵を管理する手段と、前記ネットワークに属するホストの公開鍵とドメイン名とを対応付けて格納したデータベースとを持ち、第1のホストからのドメイン名の情報による第2のホストの公開鍵の問い合わせを受けたとき、前記公開鍵管理手段が前記データベースを参照することにより、前記ドメイン名に対応する第2のホストの公開鍵の情報を前記第1のホストに応答することを特徴とする公開鍵管理方法。

2. 前記DNSサーバは、第1のホストから第2のホストの公開鍵の問い合わせを受けたとき、自サーバ内の前記データベースの中に問い合わせのドメイン名に対応するエントリがない場合、他の公開鍵管理手段とデータベースとを備えた他のDNSサーバに公開鍵の解決をドメイン名の階層に沿って再帰的に委託することを特徴とするクレーム1の公開鍵管理方法。

3. 前記ホストは、前記DNSサーバに他のホストの公開鍵を問い合わせる手段を備え、セキュリティ通信開始時、前記公開鍵問い合わせ手段に通信相手となるホストのドメイン名に対応する公開鍵を前記DNSサーバに問い合わせることを特徴とするクレーム1の公開鍵管理方法。

4. クレーム1の公開鍵管理方法を実現するための、DNSサーバに設けられる公開鍵を管理する手段の機能を実行するプログラムと、ネットワークに属するホスト

SECRET

ABSTRACT OF THE DISCLOSURE

階層構造のドメイン名の構成を持ち、そのドメイン名とアドレスとの対応を管理するDNSサーバが階層毎にあるネットワークにおいて、公開鍵を管理するモジュールとネットワークに属するホストの公開鍵とドメイン名との対応を示すデータベースを各DNSサーバに設ける。2つのホストがセキュリティ通信を開始するとき、一方のホストが前述の機能拡張したDNSから通信相手のホストの公開鍵を自動的に取得する。このとき、公開鍵問い合わせパケットの中にホストが信用するDNSサーバの名前を入れさせ、このホストが指定するDNSサーバが、公開鍵応答パケットに電子署名を付ける。ホストは、この電子署名により公開鍵応答パケットにある公開鍵が信用できるかどうかを判定することができ、不正なホストが通信相手になりすますのを防止する。

09585358-060200

図 1

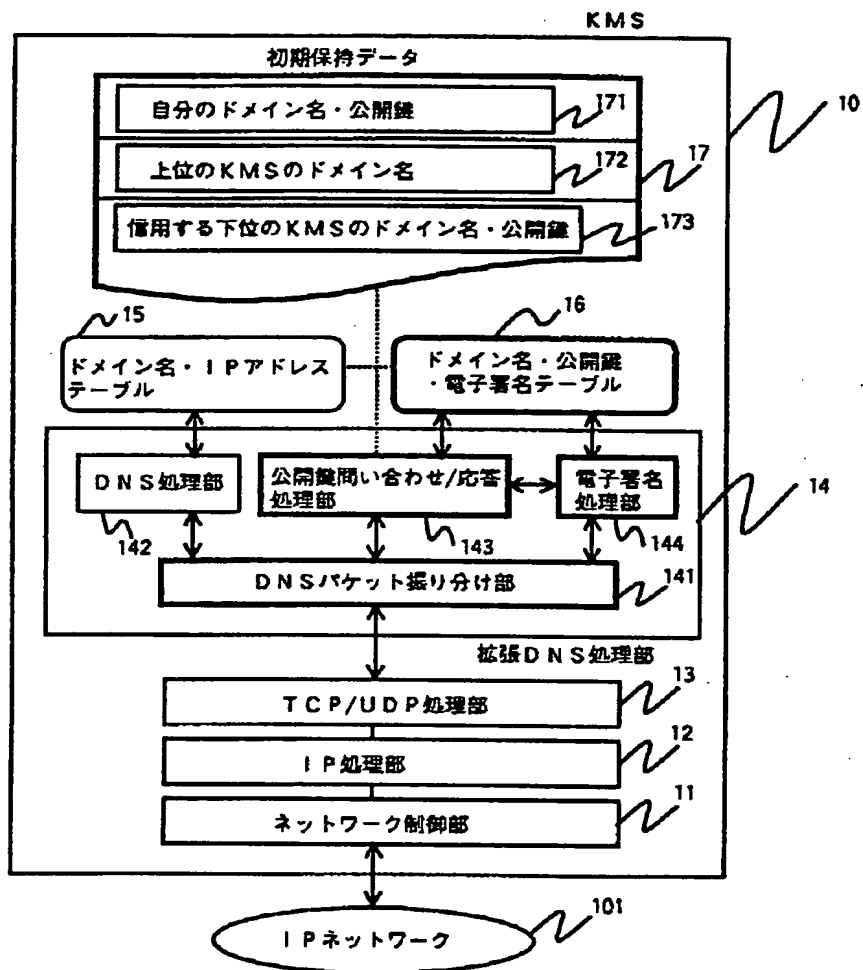


图 2

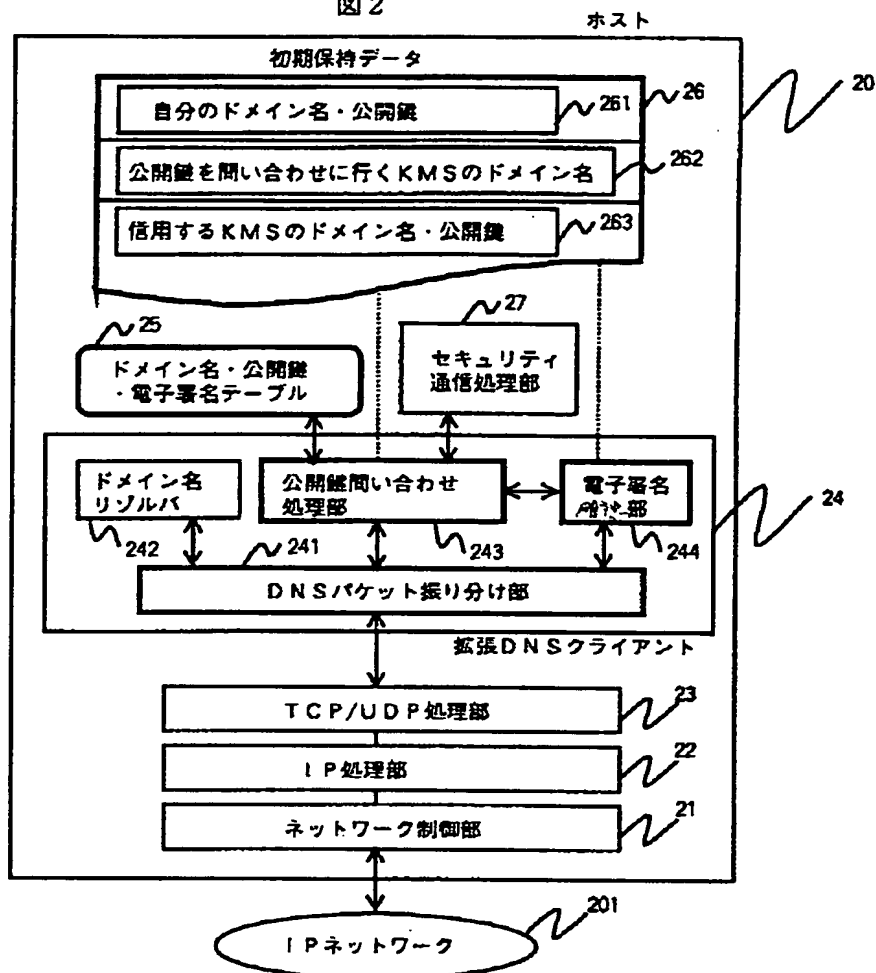


图 3

ドメイン名 ³¹	公開鍵 ³²	電子署名 ³³	電子署名を付けたKMS名 ³⁴	タイムスタンプ ³⁵

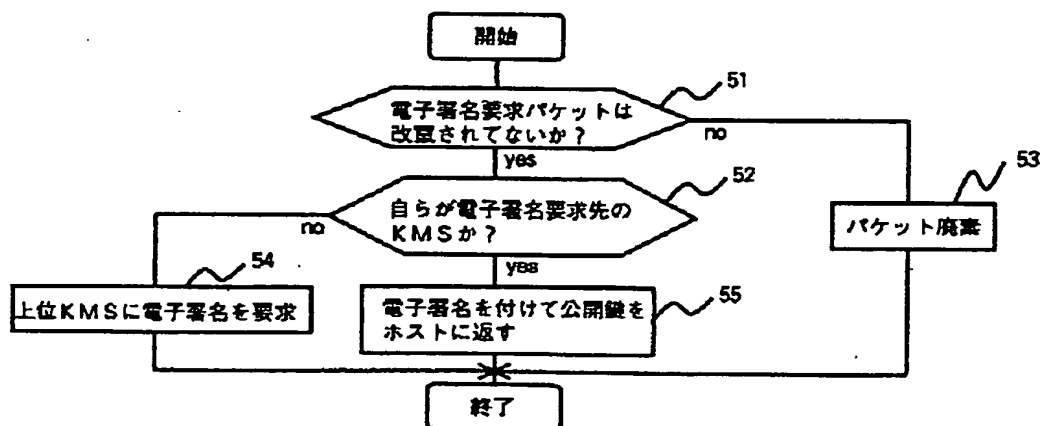
[illegible]

图 6

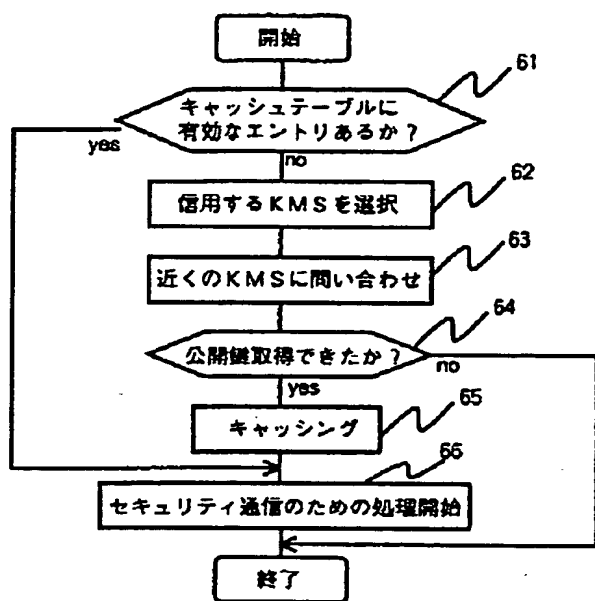


圖 7

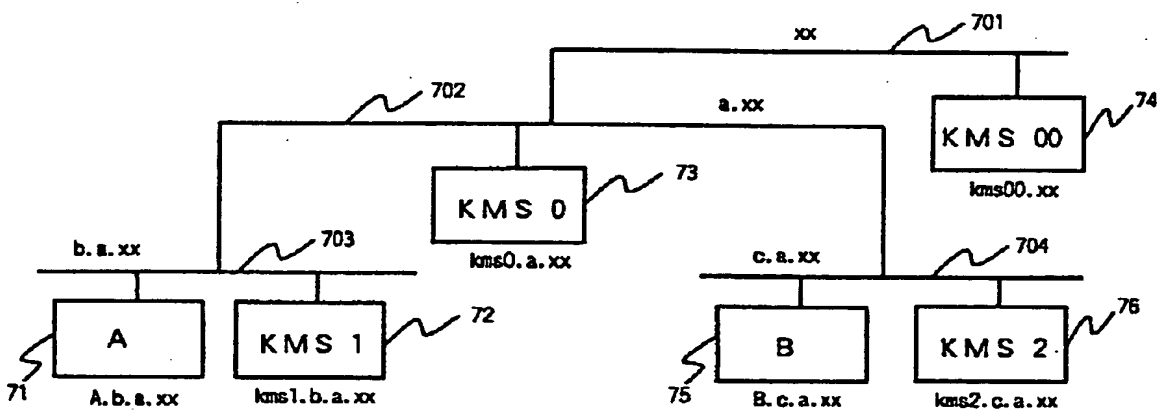
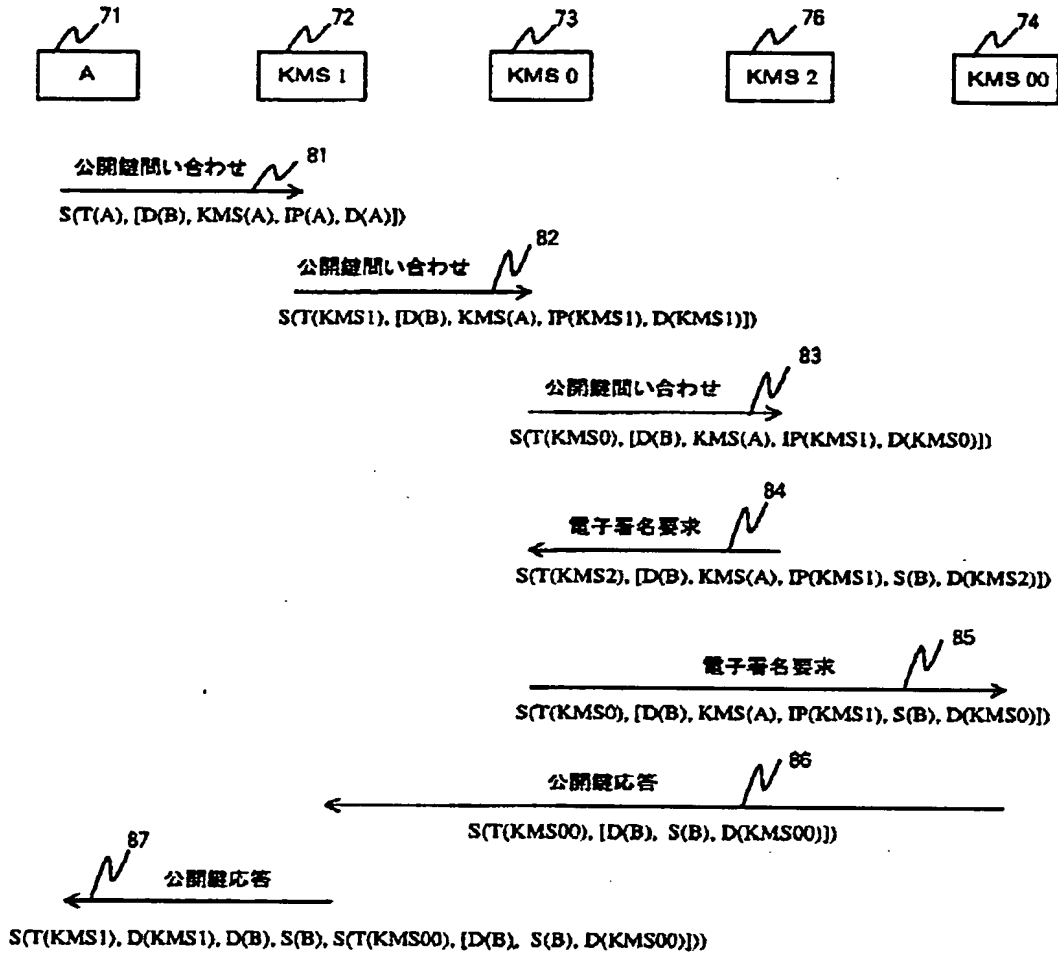


図 8



DX): Xのドメイン名

S(X): Xの公開鍵

T(X): Xの秘密鍵

IP(X): XのIPアドレス

KMS(X): Xが電子署名を要求するKMS

S(K, [a, b, c]): 鍵Kでメッセージ [a, b, c] に電子署名をつけたもの

SECRET



8

